AUSA: Timothy Wyse Telephone: (313) 226-9144

AO 106 (Rev. 04/10) Application for a Search Warrant Special Agent: Bryan Randall Telephone: (216) 701-7915

UNITED STATES DISTRICT COURT

for the

Eastern District of Michigan

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 6495 Telegraph Road, Bloomfield Township, MI 48301	Case No.	2:17-mc-51454 Assigned To : Drain, Gershwin A. Assign. Date : 10/25/2017

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See ATTACHMENT A.

located in the Eastern District of Michigan, there is now concealed *(identify the person or describe the property to be seized):*

See ATTACHMENT C.

I hereby certify that the foregoing is a certified copy of the original on file in this office.
Clerk, U.S. District Court
Eastern District of Michigan
By: Lisa Bartlett
Deputy

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC § 1960	Operating an Unlicensed Money Transmitting Business

The application is based on these facts:

See attached AFFIDAVIT.

☑ Continued on the attached sheet.

☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Bryan Randall, Special Agent HSI

Printed name and title

Sworn to before me and signed in my presence and/or by reliable electronic means.

Date: October 25, 2017

Judge's signature

City and state: Detroit MI

Mona K. Majzoub U. S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR the Eastern District of Michigan

IN THE MATTER OF THE SEARCH OF: **6495 Telegraph Road, Bloomfield Township, MI 48301**	Case No. 2:17-mc-51454 Assigned To : Drain, Gershwin A. Assign. Date : 10/25/2017

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, **Bryan Randall**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 6495 Telegraph Road, Bloomfield Township, MI 48301, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B. As further described in this affidavit and detailed in Attachment B, the purpose of this search is limited to the seizure of electronic devices in the possession of Bradley Anthony STETKIW, who will be present at the PREMISES at approximately 1900 hours on October 25, 2017.

2. I am a Special Agent with Homeland Security Investigations ("HSI") within the United States Department of Homeland Security, and have been since August of 2009. As part of my employment with HSI, I successfully completed the Federal Law Enforcement Training Center's Criminal Investigator Training Program and the Immigration and

Customs Enforcement Basic School, both of which included intensive instruction with regard to Customs laws, financial crimes and drug enforcement, including the application for, and execution of, search and arrest warrants, as well as the application for criminal complaints, and other legal process. I am currently assigned to the Dark Web Group, (hereinafter "HSI Detroit Dark Web").

3. During my law enforcement career, I have participated in investigations of and received information from other law enforcement officers targeting money launderers and unlicensed money transmitters who use virtual currency, specifically Bitcoin, to assist in the unlawful importation and distribution of contraband in the United States.

4. I have personally participated in the money laundering and unlicensed money transmitter investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation, discussions with other agents of HSI and other law enforcement officials, interviews of witnesses, and my review of relevant records and reports. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, the information was provided by an HSI agent, law enforcement officer, or witness who had either direct or hearsay knowledge of that statement, to whom I or others have spoken or whose reports I have read and reviewed. Such statements are among statements made by others and are stated in substance and in part unless otherwise indicated. Any interpretations or opinions rendered in this affidavit are based on my

training and experience in the context of the facts of this investigation. Because this affidavit is submitted for the limited purpose of establishing probable cause for the offenses listed in the criminal complaint, it does not recite all evidence gathered thus far.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

6. From in or about July 2015 up to and including in or about August 2017, the defendant, Bradley Anthony STETKIW, ran a Bitcoin exchange in the Bloomfield Hills, Michigan, area primarily using the website "LocalBitcoins" (LBC) to find customers. STETKIW would meet his customers at Tim Hortons located at 6495 Telegraph Road, Bloomfield Township, MI 48301. STETKIW advertised on LBC that he meets his customers offline at Tim Hortons located at 6495 Telegraph Road, Bloomfield Township, MI 48301. STETKIW operated under the user name "SaltandPepper", STETKIW bought sold and brokered deals in Bitcoins for cash while failing to comply with the money transmitting business registration requirements set forth in Title 31, United States Code, Section 5330. "SaltandPepper" is a high-feedback LBC user on LBC. "SaltandPepper" advertised his service directly on LBC, as exemplified by the following post:

> "I am the longest, most reliable and honest trader in Oakland County. Start this trade to arrange meeting time and coin availability.

Meeting only at:

Tim Hortons
6495 Telegraph Road
Bloomfield Twp. MI 48301

The location is at Maple (15 mile) and Telegraph.

Transactions not completed within 12 hours are subject to cancellation."

7. Based on a subpoena for phone records and undercover bitcoin purchasing operations, I learned that the user of telephone number (248) 891-5609 is the defendant, Bradley A. STETKIW. During undercover operations in the past the man using cell phone number (248) 891-5609 identified himself to the UCA's as "Brad." An NLETS query resulted in obtaining a driver's license photo, full name, date of birth and full address of STETKIW. The query reported the following:

Bradley Anthony STETKIW, DOB: 01/19/1965, 740 Cortwright Street Pontiac, MI 48340.

8. 2015 Oakland County Tax records list Bradley A. STETKIW as the owner of the property located at 740 Cortwright, Pontiac, MI 48340.

9. Early records checks show STETKIW as the registered owner of a 2005 Chrysler Pacifica (VIN 2C4GM684X5R549473) bearing Michigan plate BGF7260. The vehicle is registered to 740 Cortwright, Pontiac, MI 48340. During a more recent

undercover purchase of bitcoin we learned that STETKIW has since changed the plate on the Pacifica. The new Michigan plate is DQH7879 and that plate is also registered to 740 Cortwright, Pontiac, MI 48340.

10. Clear reports and a copy of STETKIW's Michigan driver's license along with the video taken from the undercover purchases of Bitcoin establish that Bradley Anthony STETKIW aka "Brad" and "SaltandPepper" are multiple names for the same individual.

11. Based on undercover transactions conducted in this investigation, I know that a typical Bitcoin purchase from STETKIW worked as follows:

a. The customer would contact STETKIW through either LBC message or via text message requesting to buy a certain amount of bitcoins.

b. STETKIW and the customer would meet at Tim Hortons located at 6495 Telegraph Road, Bloomfield Township, MI 48301 and negotiate a price and STETKIW's fee/commission based off the method of payment for the bitcoin (cash, bank deposit, GreenDot MoneyPak, PayPal, etc.). STETKIW typically charged a five percent fee.

c. The customer would provide a Bitcoin address to STETKIW.

d. Upon payment, STETKIW would send bitcoins to the customer's Bitcoin address.

12. On October 23, 2017, I conducted searches for STETKIW on FinCEN's MSB Registrant Search webpage with negative results. This webpage contains entities that have registered as Money Services Businesses pursuant to the BSA regulations at 31 CFR 1022.380(a)(f). Among other requirements, individuals acting as MSBs must register with FinCEN. STETKIW has not registered as an MSB with FinCEN. 740 Cortwright Pontiac, MI returns negative results when ran through FINCEN's MSB search tool.

13. HSI UCAs, in a total of six undercover meets, purchased approximately 126.07814879 Bitcoins for $56,700(USD) from STETKIW. During all of the transactions STETKIW would meet the UCAs at Tim Hortons located at 6495 Telegraph Road, Bloomfield Township, MI 48301. There were a total of 26 Bitcoin Transactions between STETKIW and the UCAs. STETKIW charged the UCAs a percentage of the total cost to sell the bitcoins to the UCA for cash and for the UCAs to remain anonymous. STETKIW also brokered the deal between the UCAs an out-of-state Bitcoin seller that subsequently sold the UCA $35,000.00 worth of Bitcoin as an unlicensed money remitter. In the beginning one of the UCAs initially contacted STETKIW through LBC and subsequently corresponded primarily with STETKIW via text message. All six of the meetings took place at a Tim Horton's in Bloomfield Hills, MI. The following is a breakdown of the meetings and certain information obtained each transaction:

a. August 18, 2015, purchase of 1.81331156 bitcoins for $500:

i. STETKIW told UCA that STETKIW normally charges 10 percent

above actual bitcoin market rate to do a transaction outside of Localbitcoins.com but that he would do 9% direct to the UCA phone.

ii. UCA's explained that they would need more bitcoins in the future and asked STETKIW what his maximum amount would be. STETKIW stated that he could sell up to $2,500.00(USD) per person, per day. STETKIW asked the UCA's: "Were you thinking of more than that?" STETKIW then stated that he could do $2,500.00(USD) to UCA1 and $2,500(USD) to UCA2 in the same day. STETKIW, then also stated that the UCA's could bring more people and he could sell $2,500.00(USD) to each person. The UCA's asked "who regulates the $2,500.00?"

iii. STETKIW replied "That's a limit I've set just to make, trying to make things comfortable." The UCA's asked if they built a relationship could STETKIW help them out. STETKIW replied "There's been a lot of bullshit law enforcement stuff with people getting, Bitcoin sellers, getting arrested for money laundering." The UCA's stated, "That's not money laundering right, I'm just buying it?" STETKIW replied "They consider it money laundering over a certain amount transaction." The UCA's asked how much that was. STETKIW stated "That I don't, the law varies everywhere."

iv. UCA's stated that they normally used Western Union. STETKIW replied that Western Union wants ID to send money, they want ID to receive money and agreed with the UCA's that the fees were extremely high.

v. STETKIW stated "I don't know how many people you want to bring into your circle." Then added, that was all he could do, that he didn't feel comfortable doing any more than that, but pointed out that it was per person, per day, and that the UCA's could meet him at 11:45 and do one trade and then after midnight do another trade.

vi. STETKIW stated, "Just, I'm just going to say this and don't tell me what you're doing with your coin because if you do, and it's something bad, then I can't sell it to you." The UCA's replied "Well your version of bad, and my version of bad are probably different." STETKIW replied "Then just don't say anything okay? That's how it goes." The UCA's replied "If you're willing to work with me, I'm willing to work with you" STETKIW replied "That's the way we have to work."

vii. The UCA's stated "hopefully this goes nice and smooth, and like I said, uh, I should probably know in what like, 2 weeks to get it, maybe 3 to get rid of it and then maybe like a month I'd get a hold of you." STETKIW told the UCA's that was okay, that he's around and that he has been selling for 2 years and doesn't see any quitting coming up anytime soon.

b. October 20, 2015, purchase of 34.92068338 bitcoins for $10,000.00:

i. STETKIW asked the UCA's "You think I'd draw too much attention if I brought one of those bill counters in here?" The UCA's stated that they were not comfortable with having that much money being on the table; STETKIW stated "Like I

said, I've been coming down here a long time and I know they don't keep, they don't keep their video more than a few days."

ii. STETKIW stated "Let me break for a minute, the only thing I suggest to you guys, as you're riding around in the car with that kind of money, hide it, somewhere in the car, like under the spare tire or something the police aren't going to see. Because if you get pulled, let's just say you get pulled over and things get out of hand, they're going to tell you, well if you can't account for that we're seizing it. And it's legal for them to do that. Money seizure laws and stuff like that."; The UCA's asked STETKIW what he did with it and he replied "I've got a way of doing it, I'm not going to tell you how."

c. March 22, 2016, purchase of 32.12238142 bitcoins for $13,700.00:

i. STETKIW stated that what started him being more careful was that, a client had shown up with a Sentry Fire Safe to do a deal which was too conspicuous for STETKIW.

ii. STETKIW asked about the UCA's receiving small bills "How do you get rid of it?" UCA2 stated "You just make small deposits over time." STETKIW stated "Well, maybe I don't want to know you get rid of it," then "cancel that question." UCA2 asked STETKIW, how do you get rid of it? STETKIW stated "Box it up." UCA2 asked about sharing ideas on how to get rid of small bills. STETKIW stated lots of stores need small bills.; UCA1 stated that he/she understood that STETKIW takes the cash and goes and buys coin but at some point the cash needs to go back into commerce and that someone

wants to do something with that cash. We have that problem, we've got a lot of cash and we can't go to the bank and deposit $80,000(USD) cash, I can, but I might get a phone call; STETKIW laughed and stated "Not over ten grand, I wouldn't do any transaction with a bank over ten."

d. April 20, 2016, purchase of 32.32635728 bitcoins for $15,000.00:

i. UCA explained that he/she wanted to do what they could with STETKIW but do the remainder with an out-of-state seller and pay STETKIW a percentage or whatever he was comfortable with. STETKIW stated "The problem with [the out-of-state seller] is that I've given that guy a shit ton of business and he doesn't seem to take care of my people as well as I'd like him to." The UCA asked "In what way?" STETKIW stated "He's unresponsive, an, just, his rates, I thought his rates were kind of high for uh thirty five thousand dollars." The UCA asked what the rates were and STETKIW stated "I think he said five and a half to six."

ii. STETKIW stated "All the business I've given him, he hasn't, he hasn't even given me a dollar worth of coin so it's kind of an annoyance factor with me too." The UCA stated "I'm not trying to cut you out of anything, I'm happy to one guy I recommended him, they trade regularly and, we're talking, it's probably way over a hundred thousand dollars by now." The UCA asked "Total?" STETKIW replied "Total, at least. And you know and he hasn't said shit. It's like, okay, well I keep sending you these people, it's probably just a courtesy to send a few dollars."

iv. The UCA asked how to contact the out-of-state-seller, STETKIW replied

"Well I've got the info for you" and pulled out a wallet from his shirt pocket. STETKIW then provided the UCA with a piece of paper with contact information.

e. August 31, 2016, purchase of 24.38074075 bitcoins for $15,000.00:

i. STETKIW told the UCA he would have to break up the sale into six separate transactions in order to prevent any one transaction from exceeding $2,500.00.

ii. STETKIW told the UCA he appreciated the fact the funds were all in $100 bills and also stated he has a money counter at his home.

iii. The UCA provided six wallet addressed to STETKIW who then made six different deposits for a total of 24.38084075 BTC.

f. August 28, 2017, purchase of 0.5146744 bitcoins for $2,500.00:

i. STETKIW met with a UCA that he had never conducted trades with in the past. Without identifying the UCA or requesting for identification information STETKIW sold the UCA 0.5146744 bitcoins. STETKIW charged the UCA points on the transaction that equaled approximately $154.13.

TIM HORTONS 6496 Telegraph Road Bloomfield Township, MI 48301

14. Multiple surveillances conducted at Tim Hortons located at 6495 Telegraph Road, Bloomfield Township, MI 48301 show STETKIW frequently meets clients in the lobby of the restaurant. STETKIW advertises on LBC that he will only meet his clients at Tim Hortons located at 6495 Telegraph Road, Bloomfield Township, MI 48301.

15. On June 16, 2016, a tracker warrant for STETKIW's vehicle was obtained and signed off on by a Magistrate Judge in the 48th District Court of the State of Michigan. On June 30, 2016, at approximately 2200 hours, HSI Detroit Special Agents installed a GPS tracker onto the red Chrysler Pacifica (Michigan License Plate: BGF 7260) which is owned and operated by STETKIW. The tracker results showed frequent trips between Tim Hortons located at 6495 Telegraph Road, Bloomfield Township, MI and 740 Cortwright Pontiac, MI 48340. From the tracker information HSI Detroit was able to note that STETKIW also made stops at Bloomfield Village Square Shopping Center, Chase Bank (Bloomfield Town Square) and Speedway gas station at Dixie Highway and North Telegraph. HSI Detroit was able to pull bank account information for STETKIW from Chase bank subsequent to documenting his notable stops.

16. During the meets with the UCAs, at Tim Hortons located at 6495 Telegraph Road, Bloomfield Township, MI 48301, STETKIW would use electronic devices to conduct the transfer of Bitcoin from his wallet addresses to the UCAs wallet address. STETKIW conducted his business inside Tim Hortons using tablets, laptops and cell phones. The UCAs

are unable to verify whether or not the same electronic devices were used during each buy or if STETKIW used various devices.

17. Bitcoin is stored in Bitcoin wallets both online and offline. In order to access these wallets the owner of the Bitcoin must have a wallet address and a private key. A wallet address resembles a VIN. It is a sequence of letters and numbers and can contain up to 34 characters. Wallet addresses can also come in the form of a QR code which STETKIW and the UCAs have presented to one another scan to initiate the transfer of Bitcoin from STETKIW's wallet to the UCA's wallet. This was done using apps on both the UCA's phone and STETKIW's phone.

18. I know that STETKIW will be present at the subject premises on October 25, 2017 at approximately 1900 hours because I messaged STETKIW on LBC asking him to meet so that to purchase $10,000.00(USD) worth of bitcoins. STETKIW responded, and on October 25, 2017 agreed to meet at the subject premises at 1900 on this date to conduct a transaction in which he would sell $5,000(USD) worth of bitcoins.

TECHNCAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of

transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images.

This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that

are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "Wi-Fi" networks, or otherwise. Tablets

typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

a. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and

international borders, even when the devices communicating with each other are in the same state.

b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

c. Peer-to-peer (P2P) is a decentralized communications model in which each party has the same capabilities and either party can initiate a communication session. Unlike the client/server model, in which the client makes a service request and the server fulfills the request, the P2P network model allows each node to function as both a client and server.

d. TOR directs Internet traffic through a free, worldwide, volunteer network consisting of more than six thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using TOR makes it more difficult for Internet activity to be traced back to the user; this includes visits to Web sites, online posts, instant messages, and other communication forms.

e. "AlphaBayMarket" was operated for over two years on the dark web and was used to sell deadly illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other

computer hacking tools, firearms, and toxic chemicals throughout the world. AlphaBay was the world's largest underground marketplace of the dark net, providing an avenue for criminals to conduct business anonymously.

f. Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an upper case letter B) to label the protocol, software, and community, and "bitcoin" or "bitcoins" (with a lower case b) to label units of the currency and that practice is adopted here.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

14. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

15. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

16. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, that belongs to STETKIW and that is used in the commission of the crime of unlicensed money remitting, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of other evidence related to this investigation, I am aware that cell phone and computer equipment was used to generate wallet addresses used in the unlicensed money remitting scheme. There is reason to believe that there is a computer system and cell phones used in the undercover transactions currently located on the PREMISES.

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that

establishes how computers and cellular phones were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus

enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a

computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, wallet addresses, wallet apps or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

18. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media.

Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or

knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

20. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B. HSI Detroit has made arrangements with STETKIW to meet him at Tim Hortons located at 6495 Telegraph Road, Bloomfield Township, MI 48301 on Wednesday, October 25, 2017 at 1900 hours to purchase $5,000 worth of Bitcoin.

Respectfully submitted,

BRYAN RANDALL
Special Agent
Homeland Security Investigations

Subscribed to before me and signed in my presence and/or by reliable electronic means.

Dated: October 25, 2017

HONORABLE MONA K. MAJZOUB
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is Tim Hortons located at 6495 Telegraph Road, Bloomfield Township, MI 48301, further described as a commercial business that shares a building with a gas station and is located on the corner of Telegraph and Maple. The building sits on the northeast corner of Telegraph and Maple.

ATTACHMENT B

Property to be seized

1. All records, in whatever form they may be kept, relating to violations of **Title 18, United States Code, Section 1960**, those violations involving **Bradley A. STETKIW** and occurring after **July 2015**, including:

   a. Records and information relating to the selling of Bitcoin;

   b. Records and information relating to wallet addresses, including any cryptographic keys, in any form-used to access those addresses through any computer programs or online bitcoin exchanges.

   c. Bitcoin wallets, wallet addresses, hardware wallets (such as trezor or ledger devices), private keys, wallet recovery seeds, usernames, passwords, mnemonic pins, PGP keys and 2FA devices.

   d. Records and information relating to cryptocurrency exchanges used by STETKIW;

   e. Records and information relating to dark web market place purchases.

   f. Records and information relating to money received from the sale of Bitcoin.

2. United States Currency or other monetary instruments.

3. Bitcoin. Seizure of bitcoin will be effectuated by (1) identifying bitcoin wallets and their cryptographic keys through the seizure of information described in Paragraph 1, supra, and (2) transferring bitcoin to a government-controlled wallet.

4. Computers, phones, tablets, and storage media in the possession, custody, or control of Bradley A. STETKIW used as a means to commit the violations described above, including violations of Title 18, United Stats Code, Section 1960 or any such devices that may contain any communications with buyers and sellers of bitcoins.

5. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

k. contextual information necessary to understand the evidence described in this attachment.

6. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.